



UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

"Device A" - A black smartphone, unknown make, with an AT&T logo on the back

Case No.

23-M-443 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before **9-28-23** *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 9-14-23. 10:00 am

Stephen C. Davis
Judge's s

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

| Return | | |
|---|---------------------------------|--|
| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
| Inventory made in the presence of : | | |
| Inventory of the property taken and name(s) of any person(s) seized: | | |
| Certification | | |
| <p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <div style="text-align: center; margin-bottom: 10px;"> <p>_____</p> <p><i>Executing officer's signature</i></p> </div> <div style="text-align: center;"> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div> </div> | | |

ATTACHMENT A

1. The property to be searched is described as follows:

a. A black smartphone, unknown make, with an AT&T logo on the back,
hereinafter referred to as “**Device A**.”

2. **Device A** is currently secured at 345 W. Saint Paul Avenue, Milwaukee, Wisconsin.

This warrant authorizes the forensic examination of **Device A** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on **Device A** described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, including, but not limited to:
 - a. Preparatory steps taken in furtherance of these crimes;
 - b. Lists of customers and related identifying information;
 - c. Types, amounts, and prices of drugs trafficked and money laundered as well as dates, places, and amounts of specific transactions;
 - d. Any information related to sources of drugs and money and co-conspirators (including names, addresses, phone numbers, or any other identifying information);
 - e. Any information recording schedule or travel;
 - f. All bank records, checks, credit card bills, account information, and other financial records;
 - g. Any audio, video, and/or photograph(s) files on the phone of criminal activity or of evidentiary value, including those depicting possession of drugs or money;
 - h. All voicemail and call records;
 - i. All text messages and call history;
 - j. All social media sites used and applications for social media sites;
 - k. All internet activity;
 - l. All location data including from the phone and/or from any downloaded applications;
 - m. Any evidence related to either the ownership, purchase, or possession of drugs, money, or other assets; and
 - n. Records of Internet activity, including browser history, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Evidence of user attribution showing who used or owned **Device A** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the USPIS may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)"Device A" - A black smartphone, unknown make, with
an AT&T logo on the backCase No. **23-M-443 (SCD)**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section | Offense Description |
|-----------------------|---|
| 21 U.S.C. § 841(a)(1) | Distribution of a controlled substance, unlawful use of a communication facility, |
| 21 U.S.C. § 843(b) | and conspiracy. |
| 21 U.S.C. § 846 | |

The application is based on these facts:

Please see attached affidavit, which is hereby incorporated by reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Tyler Fink

Digitally signed by Tyler Fink
Date: 2023.09.13 15:00:36 -05'00'

Applicant's signature

Tyler Fink, Inspector, USPIS

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone _____ (specify reliable electronic means).

Date: 9-14-23

 Judge's signature
City and state: Milwaukee, Wisconsin

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT

I, Tyler Fink, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a United States Postal Inspector, assigned to the United States Postal Inspection Service (“USPIS”) Domicile in Milwaukee, Wisconsin as well as being placed on the High Intensity Drug Trafficking Area (“HIDTA”) Interdiction Task Force. I have been employed as a full-time law enforcement officer since 2014.

3. The USPIS is the primary investigative arm of the United States Postal Service (“USPS”) and is charged under Title 18, United States Code, 3061 with the enforcement of laws governing the use and movement of the United States Mail, including, but not limited to, the misuse and fraudulent schemes involving the mail, crimes relating to mail fraud, identity theft, and narcotics trafficking involving the U.S. Mail.

4. I am currently assigned to the USPIS Milwaukee Office, Multi-function team, as well as being placed on the High Intensity Drug Trafficking Area (“HIDTA”) Interdiction Task Force. The USPIS Milwaukee Office investigates USPS customers involving narcotics, prohibited mailings, controlled substances, and other matters related to the Postal Service. The Milwaukee

office's team has intercepted numerous parcels, which were found to contain narcotics or proceeds of narcotics trafficking and other criminal activity.

5. I have participated in numerous complex narcotics investigations which involved violations of state and federal controlled substances laws including Title 21, United States Code, Sections 841(a)(1), 846 (possession with intent to distribute a controlled substance and conspiracy to possess with intent to distribute a controlled substance), 843, (unlawful use of a communication facility (including the mails) to facilitate the distribution of a controlled substance) and other related offenses. I have had both formal training and have participated in numerous complex drug trafficking investigations, including ones using wiretaps. More specifically, my training and experience includes the following:

- a. I have used informants to investigate drug trafficking. Through informant interviews, and extensive debriefings of individuals involved in drug trafficking, I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin and throughout the United States;
- b. I have also relied upon informants to obtain controlled substances from dealers and have made undercover purchases of controlled substances;
- c. I have participated in several search warrants where controlled substances, drug paraphernalia, and drug trafficking records were seized;
- d. I have extensive experience conducting street surveillance of individuals engaged in drug trafficking. I have participated in the execution of numerous search warrants where controlled substances, drug paraphernalia, and drug trafficking records were seized;
- e. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, cocaine, cocaine base (unless otherwise noted, all references to crack cocaine in this affidavit is cocaine base in the form of crack cocaine), ecstasy, fentanyl, and methamphetamine. I am familiar with the methods used by drug dealers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances;

- f. I am familiar with the language utilized over the telephone to discuss drug trafficking, and know that the language is often limited, guarded, and coded;
- g. I know that drug traffickers often use electronic equipment and wireless and landline telephones to conduct drug trafficking operations;
- h. I know that drug traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion and control, firearms, ammunition, and records or receipts pertaining to such;
- i. I know large-scale drug traffickers often purchase and/or title their assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;
- j. I have been assigned to court-authorized wiretaps and have been trained to operate the equipment utilized to conduct such operations;
- k. I know that drug traffickers often put their telephones in nominee names in order to distance themselves from telephones that are utilized to facilitate drug trafficking; and
- l. I know that drug traffickers often use drug proceeds to purchase assets such as vehicles, property, and jewelry. I also know that drug traffickers often use nominees to purchase and/or title these assets in order to avoid scrutiny from law enforcement officials.

4. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware and software that are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

5. I have participated in several narcotics and firearms trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. On many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

6. I am currently participating in an investigation of cocaine trafficking occurring in the Milwaukee, Wisconsin area. I am familiar with the facts and circumstances regarding this investigation as a result of my personal participation in this investigation, and my review of reports prepared by, and information obtained from, other federal, state, and local law enforcement agents and officers, all of whom I believe to be truthful and reliable.¹ This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1) (Distribution and Possession with Intent to Distribute a Controlled Substance), 843(b) (Unlawful Use of a Communication Facility (including the mails) to Facilitate the Distribution of a Controlled Substance) and 846 (conspiracy to possess with intent to distribute a controlled substance) have been committed, are being committed, and will be committed by others not yet identified. There is also probable cause to

¹ Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

believe that the location information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

9. The property to be searched is described as follows:
 - a. A black smartphone, unknown make, with an AT&T logo on the back, hereinafter referred to as “**Device A**.”
10. **Device A** is currently located at 345 W. Saint Paul Avenue, Milwaukee, Wisconsin.
11. The applied-for warrant would authorize the forensic examination of **Device A** for the purpose of identifying electronically stored data more particularly described in Attachment B.

PROBABLE CAUSE

12. On June 16, 2023, Postal Inspectors in Puerto Rico determined the following parcel to be suspicious and removed it from the mail stream: USPS Priority Mail parcel 9505514584063167475717 (“SUBJECT PARCEL”). SUBJECT PARCEL was a parcel weighing approximately 15 lbs. 3 oz. The shipping label for SUBJECT PARCEL indicated it was from “Jose Colon HC-02 box 7859-5 barrio Quenbrada Baceloneta P.R. 00617”. SUBJECT PARCEL bore a handwritten label addressed to “Ivan Cruz Ortiz 845 N 26th St Apt #213 Milwaukee Wisconsin 53233”. SUBJECT PARCEL was postmarked on June 16, 2023, in Garrochales, Puerto Rico 00652 at approximately 9:34 AM. The postage paid was \$73.50.

13. Postal Inspector Sigfredo Martinez applied for and received a federal search warrant SUBJECT PARCEL. The search warrant was issued on June 22, 2023, by U.S. Magistrate Judge Bruce J. McGiverin in the District of Puerto Rico.

14. Upon executing the search warrant on SUBJECT PARCEL, on June 22, 2023, case agents discovered the parcel contained **Device A** and approximately 2,075 of a white powdery substance, which field tested positive for the presence of cocaine.

15. Case agents are aware, based on their training and experience, drug traffickers will frequently use cell phones to communicate with fellow co-conspirators and will provide cell phones in nominee names in order to distance themselves from telephones that are utilized to facilitate drug trafficking.

16. After requesting case agents in Puerto Rico ship the SUBJECT PARCEL and all of the evidence it contained to me for further investigation, I received these items on September 12, 2023.

17. Case agents are aware, based on their training and experience, of numerous sophisticated techniques used by drug traffickers in furtherance of their drug trafficking activities. In this investigation, the unknown subject who shipped SUBJECT PARCEL utilized several of these techniques including using a fictitious names for the sender and recipient of SUBJECT PARCEL, paying for the SUBJECT PARCEL postage in cash, secreting the suspected cocaine inside of a hollowed out electrical tool, and attempting to provide the recipient of the SUBJECT PARCEL with a cell phone suspected to be in a nominee name on the cellular phone account to avoid law enforcement identification of the user of the devices. Therefore, case agents believe the subjects not yet identified involved with the shipment of **Device A** and the suspected cocaine are sophisticated drug traffickers who participated in the shipment cocaine for the distribution of narcotics to drug traffickers in the Eastern District of Wisconsin.

18. Case agents believe the subjects not yet identified used **Device A** and their cell phones to facilitate drug trafficking and evidence of drug trafficking may likely be stored and recorded on **Device A**.

19. Through my training, experience, and discussions with other experienced law enforcement officers, I am familiar with the ways in which drug traffickers and money launderers conduct their unlawful trade, including their methods of distribution, their use of communication devices, their use of coded communications to conduct their transactions, the employment of counter surveillance, their use of false or fictitious identities, and their use of various forms of electronic devices to store and/or conceal illegal activity.

20. Based upon my training and experience, I know individuals involved in drug trafficking and money laundering frequently use cellular telephones to maintain contact and arrange transactions with their sources and customers of and co-conspirators in the distribution of controlled substances and money laundering. I have also found it very common for crime suspects to use their cellular telephones to communicate aurally or via electronic message in “text” format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs.

21. Based on my training and experience, I am aware that individuals involved in trafficking of controlled substances and money laundering often possess multiple cellular devices to compartmentalize their illegal activity and to avoid law enforcement detection.

22. Based upon my training and experience, I believe it is common for crime suspects who possess illegal controlled substances to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal controlled substances and proceeds

of drug trafficking. Furthermore, I believe it is common for these photographs and visual depictions to be kept and maintained on their cellular devices.

23. Based upon the facts described above, to include (1) my knowledge of and experience confirming the prolific use of electronic devices to facilitate the possession and trafficking of controlled substances and money laundering; (2) approximately two kilograms of suspected cocaine were seized from SUBJECT PARCEL; and (3) **Device A**, a cellular phone, was recovered from within SUBJECT PARCEL, there is probable cause to believe that a search of the information contained within **Device A** will produce evidence of a crime, namely evidence related to the possession and trafficking of a controlled substance.

24. **Device A** was seized by the USPIS during the execution of a search warrant on June 22, 2023.

25. **Device A** is currently secured at the USPIS Milwaukee Domicile, 345 W. Saint Paul Avenue, Milwaukee, Wisconsin. In my training and experience, I know that **Device A** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when **Device A** first came into the possession of the USPIS.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call

log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna

receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the **Device A** has the capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, and all have the ability to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **Device A** was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on **Device A** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of **Device A** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of **Device A** to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine the device once in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of **Device A** described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

1. The property to be searched is described as follows:

a. A black smartphone, unknown make, with an AT&T logo on the back,
hereinafter referred to as “**Device A**.”

2. **Device A** is currently secured at 345 W. Saint Paul Avenue, Milwaukee, Wisconsin.

This warrant authorizes the forensic examination of **Device A** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on **Device A** described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, including, but not limited to:
 - a. Preparatory steps taken in furtherance of these crimes;
 - b. Lists of customers and related identifying information;
 - c. Types, amounts, and prices of drugs trafficked and money laundered as well as dates, places, and amounts of specific transactions;
 - d. Any information related to sources of drugs and money and co-conspirators (including names, addresses, phone numbers, or any other identifying information);
 - e. Any information recording schedule or travel;
 - f. All bank records, checks, credit card bills, account information, and other financial records;
 - g. Any audio, video, and/or photograph(s) files on the phone of criminal activity or of evidentiary value, including those depicting possession of drugs or money;
 - h. All voicemail and call records;
 - i. All text messages and call history;
 - j. All social media sites used and applications for social media sites;
 - k. All internet activity;
 - l. All location data including from the phone and/or from any downloaded applications;
 - m. Any evidence related to either the ownership, purchase, or possession of drugs, money, or other assets; and
 - n. Records of Internet activity, including browser history, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Evidence of user attribution showing who used or owned **Device A** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the USPIS may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.